Abstract

A secure file transfer system which, in its preferred embodiments, uses a Java applet sent to a client computer from a server computer to double encrypt files sent from the client computer to the server computer. Once a file is sent to the server, the system notifies a recipient that a secure document awaits pickup. The system preferably uses a public shared key agreement scheme for one method of encryption and an elliptical encryption scheme for the other. The applet comes to the client computer with a shared secret key for the public key scheme and all parameters required for the elliptical encryption scheme. Upon receiving a request for secure transfer, the server sends the applet with the encryption parameters to the client machine, which must be running a client-side application or a Java-enabled browser. The applet prompts the user for the file to be transferred and encrypts the file with the elliptical encryption method. The applet then sends the encrypted file to the server in blocks, encrypting each block with the public key scheme as it is sent. The system decrypts the blocks and reassembles them into the encrypted file and then notifies the recipient of the file's presence.